

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Applicant(s): INOUE, et al

Serial No: 08/904,137

Filed: July 31, 1997

Title: PPROGRAM WRITABLE IC CARD AND METHOD THEREOF

Group: 2132

Examiner: G. Barron

COPY

APPEAL BRIEF

Assistant Commissioner
for Patents
Washington, D.C. 20231

August 19, 2002

Sir:

The following is an Appeal of the rejection set forth in the Office Action dated December 17, 2001.

REAL PARTY IN INTEREST

The Real Party in interest in this Appeal is Hitachi, Ltd., and Hitachi Video and Information Systems, Inc., as evidenced by an Assignment filed on July 31, 1997 and recorded on Reel 8662 and Frame 0526.

RELATED APPEALS AND INTERFERENCES

On information and belief there are no other appeals and interference which will directly affect or be directly affected by or having any bearing on the Boards decision in the pending appeal.

STATUS OF CLAIMS

Claims 20-38, 51-58, 71-87, 93, and 94 stand rejected under 35 USC §102(b) as being anticipated by Hirokawa et al (U.S. Patent No. 4,827,512).

STATUS OF AMENDMENTS

An Amendment was filed on even date amending claims so as to clarify that the second program being input to the IC card have encrypted based on an encryption key as discussed during the interview of June 12, 2002. It was agreed during the interview that this Amendment would accurately describe the encryption of the second program being described in the claims and that such Amendment would be entered. The Examiner indicated that this Amendment would not affect the rejection of the claims as set forth in the December 17, 2001 Office Action. This amendment is reflected in the claims as set forth in the attached Appendix.

CONCISE SUMMARY OF INVENTION

Appellants' invention is directed to a program writable IC card and method which is particularly useful for permitting new programs to be added to the IC card to cause the IC card to perform new functions not previously stored in the IC card while maintaining high security on the IC card. By use of Appellants' invention new functions can be securely added to the card, for example, by the card issuer or under instruction from the card issuer. These new added functions need not be part of the IC card as originally produced.

Thus, by use of the features of the present invention an IC card can be subjected to various customization processes to add other functions to the card as

needed while still maintaining high security on the IC card, thereby preventing the unauthorized adding of functions to the IC card.

A disadvantage of allowing new functions to be added to the IC card is that the security of the card could be compromised. Namely, one could add a function to the card which could, for example, cause unauthorized transactions to occur. These unauthorized transactions could, for example, include the unauthorized transfer of money from one account to another account.

Appellants' invention as recited in the claims overcomes the above described disadvantage permitting new functions to be added to the card with reduced risk. Appellants' invention accomplishes this by providing an IC card having a structure such as that illustrated, for example, in Fig. 1 of Appellants' application.

As illustrated in Fig. 1 of the application, Appellants' invention provides a program writable IC card which includes a microprocessor 1, and a first memory (program ROM) 3 which stores both a first program (IC card function program) 3A to be executed by the microprocessor 1 to control the IC card and a decryption program (write control program having decryption program) 3B, executable by the microprocessor 1, having a decryption function for decrypting an encrypted program.

The first memory 3 is a Read Only Memory (ROM) which is not rewritable. The program writable IC card also includes a second memory (memory for writing) 4 which can store a second program executable by the microprocessor 1 and a connector 2 for electronic connection between the IC card and an external device.

The microprocessor 1, connector 2, and the first program 3A are components for executing the original instructions of the first program programmed in the IC card.

An external instruction can be given to the microprocessor 1 via the connector 2 and

the IC card performs an operation responsive to the external instruction. The IC card function program 3A when executed is responsive to a write command given to the IC card via the connector 2 so as to activate the write control program 3B. The write control program 3B has a decryption function, and when activated by the write command requires that communications with the IC card to add a second program be conducted with the second program being encrypted using the appropriate encryption key. The decryption function serves to decrypt the encrypted second program being added to the IC card and the decrypted second program is stored in the second memory for later direct execution by the microprocessor 1.

ISSUES PRESENTED FOR REVIEW

Whether claims 20-38, 51-58, 71-87, 93, and 94 are unpatentable over Hirokawa et al under 35 USC §102(b).

GROUPING OF CLAIMS

Each of the claims should be considered by the Board individually and separately so as not to stand or fall together.

ARGUMENTS

With respect to the rejection of claims 20-38, 51-58, 71-87, 93, and 94 as being unpatentable over Hirokawa et al under 35 USC §102(b) the following is provided:

The features of Appellants' invention recited in the claims are not taught or suggested by Hirokawa.

Hirokawa teaches a programmable portable electronic device namely an IC

card. The IC card includes a memory area which is divided into a system program area and a user program area. According to Hirokawa a command text message and a response text message transmitted between the IC card and a host system (terminal) includes a flag indicating whether the text of the message is to be written in the user program area or the system program area. The memory area also includes a data area in which a conversion table is stored having a plurality of entries each including a function code and a start address of a program corresponding to the function code. The conversion table is used as a look-up table so as to decode function codes input to the IC card. As per Hirokawa, a function code input to the IC card is decoded in a manner to point to the start address of a program that performs the desired function when executed.

As taught by Hirokawa the system program area stores common processing functions for the various users including an input/output function to input or output data to or from the data area, an arithmetic operation function, and an input/output function to input or output programs to or from the user program area, etc. These common processing functions are stored during the manufacture of the IC card.

Further, as per Hirokawa the user program area stores various functions which can be added by the user so as to customize the IC card to the user. The functions added by the user are stored in the user program area under control of a control program stored in the system program area.

Hirokawa discloses three different embodiments. The first and second embodiments are directed to steps performed when a new function is added by the user. The third embodiment is directed to providing an internal configuration in the IC card for implementing various basic functions in the IC card. These three

embodiments taught by Hirokawa are illustrated, for example, in Figs. 1-9 (First Embodiment), Figs. 19-24 (Second Embodiment) and Figs. 10-18 (Third Embodiment).

With respect to the First Embodiment illustrated in Figs. 1-9, Hirokawa teaches steps for adding a new function to an IC card as per the flowchart in Fig. 9. This teaching of Hirokawa is described in col. 4, lines 13-51.

Hirokawa teaches that an IC card having a structure illustrated in Figs. 2 and 3 is inserted in an IC card manipulator (terminal) 10 illustrated in Fig. 6, the internal structure of which is illustrated in Fig. 7. According to the First Embodiment taught by Hirokawa when an addition command is input to the keyboard 12 of the terminal 10 to input an object program defining a user definition function, the IC card performs the steps illustrated in the flowchart of Fig. 9. These steps, particularly with respect to the operation of adding a new function, are described in col. 4, lines 13-51 in Hirokawa.

In col. 4, lines 13-51 of Hirokawa it is described that when the user inputs an addition command to the terminal 10 to initiate the input of an object program, the CPU 11 included in the terminal 10 supplies to the CPU 3 included in the IC card a command text message indicating that a function is to be added (step 51). The command text message illustrated in Fig. 4 includes a code corresponding to the object program to be added and the object program (text) itself. The CPU 3 detects the addition mode (step 53) and performs other steps to avoid adding a duplicate function and then stores the function including the object program in the user program area (step 55). The CPU 3 then prepares a response text message so as to confirm that such function has been added (steps 57 and 59).

With respect to the Second Embodiment illustrated in Figs. 19-24, Hirokawa

teaches steps for adding a new function to an IC card as per the flowchart in Figs. 22a and 22b. This teaching of Hirokawa is described in col. 7, line 24 through col. 8, line 20.

According to Figs. 22a and 22b, Hirokawa teaches that when storing an additional function program by an external input operation, a determination is made as to whether function program addition instruction data is being input (steps 91, 93). According to Hirokawa the function program addition instruction data includes a function program addition function code, function code addition data and function program capacity data as illustrated in Fig. 19. Hirokawa teaches that CPU 3 included in the IC card refers to the function program capacity data so as to recognize the capacity of the function program to be added and the capacity of the empty program area in the user program memory area (steps 93 and 95).

According to Hirokawa, if it is determined that the capacity is sufficient and the same codes do not exist in the system program memory area, then the function code addition data is stored in the conversion table in the data area (steps 97, 101 and 105). Thus, Hirokawa teaches that the CPU 3 sends a response confirming the acceptability of the function program data and receives function program write instruction data which includes the function program (step 107, 109). The function program write instruction data has a format illustrated in Fig. 20 of Hirokawa. As per Hirokawa the function program is written to the user program area of the IC card (steps 111, 115).

As is clear from the above, although Hirokawa teaches with respect to the First and Second Embodiments a system whereby new functions can be added, there is no teaching or suggestion with respect to the First and Second Embodiments of

Hirokawa that the new function to be added, particularly the object program or function program included in the command text message or the function program write instruction data, respectively is encrypted based on an encryption key prior to being input to the IC card as recited in the claims.

Still further, there is no teaching or suggestion with respect to the First and Second Embodiments of Hirokawa that once the inputted encrypted object or function program has been decrypted, the decrypted program is stored in memory in the IC card and the decrypted program is directly executed by the CPU included in the IC card as recited in the claims.

At no point has the Examiner specifically shown where each of the above described features recited in the claims are taught or suggested by Hirokawa.

With respect to the Third Embodiment illustrated in Figs. 10-18, Hirokawa teaches a configuration in the IC card as per Figs. 10 and 11 for implementing basic functions of the IC card. The Third Embodiment taught by Hirokawa was referred to by the Examiner in the February 9, 2001 Office Action and the December 17, 2001 Office Action. This Third Embodiment taught by Hirokawa provides a configuration in the IC card including a read/write section 35, a PIN setting/collating section 37, an encrypting/decrypting section 39 and a supervisor 41. Hirokawa teaches that the supervisor 41 manages each of the above described basic functions.

Hirokawa teaches that each of the above described basic functions are implemented in an IC card having various hardware elements connected to each other in a manner as illustrated in Fig. 11. As taught by Hirokawa the IC card includes a CPU 3, a data memory area 43, a program memory 45 and a connector 2 for obtaining electrical contact with the terminal 10 illustrated in Figs. 6 and 7. The program

memory 45 includes a mask ROM and stores a control program for the CPU 3 and the data memory 43 is used for storing various data. The Examiner's attention is directed to col. 5, lines 25-31 and col. 5, lines 50-61 of Hirokawa.

In the February 9, 2001 Office Action and the December 17, 2001 Office Action, the Examiner appears to allege that the encryption/decryption section 39 taught by Hirokawa corresponds to the decryption program included in the IC card according to the present invention. The Examiner is completely in error in this regard.

Hirokawa specifically teaches in col. 5, lines 38-49 that:

"Encrypting/decrypting section 39 is a function block for encrypting communication data when data is transmitted from CPU 11 to another terminal device to protect it from being disclosed to or modified by a third party or decrypting encrypted data. Section 39 executes processing in accordance with an encrypting algorithm having a sufficient encryption strength, e.g., DES (data encryption standard). Supervisor 41 is a function block for decoding a function code with or without data input from read/writer 20 and for selecting a necessary function from the basic functions to execute it".

Thus, as is clear from the above, Hirokawa merely teaches that the encrypting/decrypting section 39 is used for encrypting communication data when the data is transmitted from CPU 11 to another terminal or for decrypting encrypted data not program as recited in the claims. In other words, CPU 11 of the terminal 10 (not the IC card) illustrated in Figs. 6 and 7 of Hirokawa may, for example, send data to the encrypting/decrypting section 39 included in the IC card so as to encrypt the data and have the encrypted data returned by the IC card to the CPU 11 of the terminal 10 for transmission to another terminal 10. Also the encrypting/decrypting section 39 could

be used for decrypting encrypted data evidently received by the CPU 11 of the terminal 10 from another terminal 10.

The key point which the Examiner seems not to recognize is that the encrypting/decrypting section 39 as taught by Hirokawa decrypts “encrypted data” not an encrypted program to be stored in the IC card as in Appellants’ invention.

Hirokawa clearly recognizes the distinction between “data” and “program” since both terms are used in Hirokawa to describe different entities. Further, the Examiner seems not to recognize is that the “decrypted data” from the encrypting/decrypting section 39 in Hirokawa is not a decrypted program directly executable and in fact executed by the CPU 3 on the IC card as in Appellants’ invention.

Taken in context, it appears from Hirokawa that the encrypted data may be data received by the CPU 11 of terminal 10 from another terminal 10, that the encrypted data is decrypted by the encrypting/decrypting section 39 on the IC card upon receipt from CPU 11 and then returned to CPU 11, and that the decrypted data is used by the CPU 11 to perform particular processes/transactions. There is no teaching or suggestion in Hirokawa that such decrypted data is stored in a second memory on the IC card nor that the decrypted data is a program directly executable and in fact executed by the CPU 3 on the IC card as in Appellants’ invention.

Further, it is quite clear from the above, that the decoding function taught by Hirokawa is merely used for decoding a function code so as to identify which of the prestored programs are to be executed according to the conversion table (look-up table) stored in the data area. There is no teaching or suggestion in Hirokawa that the decoding taught therein is truly a decoding of an encrypted program, wherein the decrypted program is executable and in fact executed by the CPU 3 on the IC card

and the encrypted program is encrypted based on an encryption key as in Appellants' invention.

In the February 9, 2001 Office Action and the December 17, 2001 Office Action, it appears that the Examiner has confused the two concepts regarding a decoding function and the encrypting/decrypting function performed by the encryption/decryption section 39 and seems to refuse to recognize that at no point is there any teaching or suggestion in Hirokawa that a decryption is performed with respect to an encrypted program, that such decrypted program is directly executable and executed by the CPU 3 included on the IC card, and that the encrypted program is encrypted based on an encryption key as in Appellants' invention.

In the February 9, 2001 Office Action and the December 17, 2001 Office Action, the Examiner points to teachings in Hirokawa at col. 1, lines 25-28; col. 5, lines 45-49; and col. 6 lines 38-43 which the Examiner alleges teaches that the "decryption function in the card allows for the encrypted program to be decrypted and used".

The teaching in Hirokawa at col. 1, lines 25-28 merely describes the well known features of an IC card wherein in order to maintain security for a function program stored on the IC card data to be processed by the program is encrypted when input to the IC card and then decrypted by the function program stored on the IC card for processing by the functions/processings implemented by the function program when executed. The key point to recognize here which the Examiner seems to overlook is that Hirokawa conforms with what is known by those of ordinary skill in the art, encrypted data is not an encrypted program, the encrypted data is simply data used during processings executed on the IC card, the encrypted is not a program to be added that is stored in the second memory of the IC card and executed by the

microprocessor of the IC card. Such encrypted data as taught by Hirokawa is not a program executable and executed by the processor on the IC card as in Appellants' invention.

There is a clear distinction between "data" used during processings performed by a program when executed and a "program" which is executable and executed by a CPU on the IC card. This distinction is clearly recited in the claims. Specifically, the claims recite that the encrypted program is decrypted by a decryption function on the IC card and such decrypted program is directly executable and executed by the processor on the IC card. Such features are not inherent nor obvious relative to the teachings at col. 1, lines 25-28 of Hirokawa.

The teachings at col. 5, lines 45-49 and col. 6, lines 38-43 of Hirokawa are merely directed to a function for decoding a function code included in command data being input to the IC card. As clearly described in Hirokawa each function code corresponds to a function program previously stored on the IC card. In order to decode such a function code Hirokawa teaches that the function code is applied to the conversion table (lookup table) in a manner so as to identify the start address of the function program corresponding to the function code. This teaching of Hirokawa is not directed to the decryption of an encrypted program which has been encrypted based on an encryption key and which when decrypted is executable and executed by the CPU included on the IC card as in Appellants' invention.

Thus, based on the above, it is quite clear that Hirokawa does not anticipate nor render the obvious the features of Appellants' invention as recited in the claims. Therefore, Appellants' respectfully request that the rejection of claims 20-38, 51-58, 71-85, 93 and 94 under 35 USC §102(b) as being anticipated by Hirokawa be

reversed.

During an interview on June 12, 2002, Appellants pressed the Examiner to point to a specific teaching in Hirokawa that supports the Examiner's allegation that Hirokawa teaches the adding of an encrypted program. In response the Examiner stated as set forth in the June 12, 2002 Interview Summary that:

"While the Examiner interpreted the Hirokawa reference as having a teaching of adding encrypted programs as the Background of the Invention section of the reference provides the context for the reference"

The relevant parts of the Background of the Invention section of Hirokawa referred to by the Examiner during the June 12, 2002 interview are col. 1, lines 18-29 which states:

"More specifically, when instruction data is input from an external device, the control element executes a decrypting program in the control program, and searches and executes a function program corresponding to the input instruction data. Thereafter, the control element outputs the result as response data to the external device.

In the conventional IC card, the function program is stored in a program memory comprising a mask ROM in or outside the control element. For this reason, if the function program for decrypting data is stored in the IC card, the encrypting method cannot be modified."

and col. 1, lines 35-38 which states:

"Therefore, strong demand has arisen for a technique for storing and executing a new function program in addition to the already stored function program."

As can be seen above these passages of Hirokawa clearly do not teach the adding of encrypted programs as recited in the claims. These passages of Hirokawa merely disclose the desire to provide a system in which new functions can be added to an IC card. The apparatus disclosed and claimed in Hirokawa is simply Hirokawa's proposed solution to satisfy this desire. However, as noted in the present Appeal Brief Hirokawa may have proposed a mechanism for adding new functions to an IC card, but this proposed solution did not consider nor was it directed to providing a mechanism in which new functions can be added in a secure manner by encrypting the program to be added based on an encryption key that can be decrypted and executed by the microprocessor on the IC card when input to the IC card. The encryption/decryption section 39 taught by Hirokawa encrypts or decrypts data used in processings performed the IC card not the new functions added to the IC card as in Appellants' invention.

Hirokawa further fails to teach or suggest numerous other features as recited in the claims, particularly the dependent claims.

For example, claim 20 recites the above described features regarding the microprocessor, first memory storing the first program and being a ROM, and a second memory for storing the second program, wherein the microprocessor decrypts the encrypted second program and stores the same in the second memory. The decrypted second program is executable by the microprocessor. The features recited in claim 20 are not taught or suggested by Hirokawa nor are they addressed by the Examiner.

Claim 21 depends from claim 20 and recites that the microprocessor performs the decrypted second program stored in the second memory. As per the above, the

decrypted second program is executable by the microprocessor. The features recited in claim 21 are not taught or suggested by Hirokawa nor are they addressed by the Examiner.

Claim 22 recites features similar to claim 20 but recites that a second memory is provided in which the second program may be written, that the microprocessor applies the decryption function to the encrypted second program and then writes a decrypted second program in the second memory according to the write control program. These features as recited in claim 22 are not taught or suggested by Hirokawa nor are they addressed by the Examiner.

Claim 23 which depends from claim 22 further recites that the program writeable IC card includes a connector which inputs the encrypted second program from outside the IC card. These features are not taught or suggested by Hirokawa nor are they addressed by the Examiner.

Claim 24 recites a program writeable IC card wherein the first memory stores a first program and a second program for decrypting an encrypted program, a second memory is able to store a third program, and an input unit inputs an encrypted third program. The second program decrypts the third program and the decrypted third program executable by the processor is stored in the second memory. These features recited in claim 24 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 25 which depends from claim 24 recites that the second program has a function for controlling the writing of a program in the second memory and the microprocessor writes the decrypted third program in the second memory according to the second program. These features recited in claim 25 are not taught or suggested

by Hirokawa nor have they been addressed by the Examiner.

Claim 26 recites a program writeable IC card similar to claim 20 but that the encrypted second program is initially supplied from outside the IC card. These features recited in claim 26 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 27 which depends from claim 20 recites that the first program performs an original function of the IC card. These features recited in claim 27 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 28 which depends from claim 22 recites features similar to that recited in claim 27. These features to the extent that they are recited with respect to claim 22 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 29 which depends from claim 24 recites features similar to that recited in claim 27. These features to the extent that they have been recited with respect to claim 24 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 30 which depends from claim 26 recites features similar to that recited in claim 27. These features recited in claim 30 to the extent that they are recited with respect to claim 26 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 31 which depends from claim 20 recites that the first program is an IC card function program for realizing an original function of the IC card. These features recited in claim 31 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 32 which depends from claim 22 recites features similar to that recited in claim 31. These features recited in claim 32 to the extent that they are recited with respect to claim 22 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 33 which depends from claim 24 recites features similar to that recited in claim 31. These features recited in claim 33 to the extent that they are recited with respect to claim 24 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 34 which depends from claim 26 recites features similar to that recited in claim 31. The features recited in claim 34 to the extent that they are recited with respect to claim 26 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 35 which depends from claim 20 recites that the first memory is read only memory which is unable to rewrite. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 36 which depends from claim 22 recites features similar to those recited in claim 35. These features recited in claim 36 to the extent that they relate to claim 22 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 37 which depends from claim 24 recites features similar to those recited in claim 35. These features recited in claim 37 to the extent that they relate to claim 24 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 38 which depends from claim 26 recites features similar to those recited

in claim 35. These features recited in claim 38 to the extent that they relate to claim 26 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 51 which depends from claim 20 recites that the first program has been stored before the second program is stored in the second memory and the second program is a new program. These features are not taught or suggested Hirokawa nor have they been addressed by the Examiner.

Claim 52 which depends from claim 22 recites features similar to those recited in claim 51. These features to the extent that they relate to claim 22 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 53 which depends from claim 24 recites features similar to those recited in claim 51. These features to the extent that they relate to claim 24 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 54 which depends from claim 26 recites features similar to those recited in claim 51. These features to the extent that they relate to claim 26 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 55 which depends from claim 20 recites that the second memory can be written only once. These features are not taught or suggested by Hirokawa nor have been addressed by the Examiner.

Claim 56 which depends from claim 22 recites features similar to those recited in claim 55. These features to the extent that they relate to claim 22 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 57 which depends claim 24 recites features similar to those recited in claim 55. These features to the extent that they relate to claim 24 are not taught or

suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 58 which depends from claim 26 recites features similar to those recited in claim 55. These features to the extent that they relate to claim 26 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 71 is directed to a processing method for a program writeable IC card wherein the method includes inputting an encrypted second program which has been encrypted based on an encryption key from outside the IC card, decrypting the encrypted second program according to the decryption program and storing a decrypted program in the second memory wherein the decrypted second program is executable by the microprocessor. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 72 which depends from claim 71 recites that the method further includes a step of executing the decrypted second program after storing the decrypted second program in the second memory. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 73 recites another processing method similar to claim 71 but that a step of executing the decrypted second program stored in the second memory is conducted. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 74 recites yet another processing method similar to claim 71 but that the second memory can be written only once. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 75 recites a writing method for an IC card including inputting an encrypted second program which has been encrypted based on an encryption key

from an external device, decrypting the encrypted second program according to the write control program and storing a decrypted second program in the writeable memory according to the write control program wherein the decrypted second program is executable by the microprocessor. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 76 which depends from claim 75 recites that the writing method further includes executing the decrypted second program after storing the decrypted second program in the writeable memory. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 77 is directed to another writing method similar to claim 75 wherein the decrypted second program stored in the writeable memory is executed. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 78 which depends from claim 71 recites that the first program performs an original function of the IC card. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 79 which depends from claim 73 recites features similar to those recited in claim 78. These features to the extent to relate to claim 73 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 80 which depends from claim 74 recites features similar to those recited in claim 78. These features to the extent to relate to claim 74 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 81 which depends from claim 75 recites features similar to those recited in claim 78. These features to the extent to relate to claim 75 are not taught or

suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 82 which depends from claim 77 recites features similar to those recited in claim 78. These features to the extent they relate to claim 77 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 83 which depends from claim 71 recites that the first program is an IC card function for realizing an original function of the IC card. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 84 which depends from claim 73 recites features similar to claim 83. These features to the extent that they relate to claim 73 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 85 which depends from claim 74 recites features similar to claim 83. These features to the extent that they relate to claim 74 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 86 which depends from 75 recites features similar to claim 83. These features to the extent that they relate to claim 75 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 87 which depends from claim 77 recites features similar to claim 83. These features to the extent that they relate to claim 77 are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 93 which depends from claim 80 recites that the second memory can be written only once. These features are not taught or suggested by Hirokawa nor have they been addressed by the Examiner.

Claim 94 which depends from claim 76 recites that the writeable memory can be written only once. These features are not taught or suggested by Hirokawa nor

have they been addressed by the Examiner.

Therefore, in light of the above, it is quite clear that the numerous features recited throughout each of the claims are not anticipated by or rendered obvious by Hirokawa nor have they been addressed by the Examiner.

Thus, based on the above, Hirokawa does not anticipate nor render obvious the features of Appellants' invention as recited in the claims. Therefore, Appellants' respectfully request that the Examiner's rejection of the claims as being anticipated by Hirokawa under 35 USC §102(b) be reversed.

SUMMARY

Appellants' submit that the Examiner's rejection of claims 20-38, 51-58, 71-87, 93, and 94 as being unpatentable over Hirokawa et al under 35 USC §102(b) is not properly founded in law and respectfully request the Board to reverse the Examiner's rejection.

To the extent necessary, applicants petition for an extension of time under 37 C.F.R. section 1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 01-2135 (Case No. 520.38929CX2) and please credit any excess fees to such Deposit Account.

Respectfully submitted,



(703) 312-6600
CIB/jdc

Carl I. Brundidge
Registration No. 29,621
ANTONELLI, TERRY, STOUT & KRAUS, LLP

APPENDIX

CLAIMS

20. (Twice Amended) A program writable IC card comprising:

a microprocessor;^①

a first memory^③ which stores both a first program to be executed by said microprocessor and a decryption program, executable by said microprocessor, having a decryption function,

wherein said first memory is a read only memory (ROM) which is not re-writable; and

a second memory^④ capable of storing a second program,

wherein said microprocessor applies said decryption function to an encrypted second program, which has been encrypted based on an encryption key, according to said decryption program and then stores a decrypted second program, which is executable by said microprocessor, in said second memory, when said encrypted second program is provided from outside the IC card.

21. (Amended) A program writable IC card according to claim 20, wherein said microprocessor performs said decrypted second program stored in said second memory.

22. (Twice Amended) A program writable IC card, comprising:

a microprocessor;

a first memory which stores both a first program which is executed by said microprocessor and a write control program, executable by said microprocessor,

having a decryption function,

wherein said first memory is a read only memory (ROM) which is not re-writable; and

a second memory in which may be written a second program,

wherein said microprocessor applies said decryption function to an encrypted second program, which has been encrypted based on an encryption key, and then writes a decrypted second program, which is executable by said microprocessor, in said second memory according to said write control program, when said encrypted second program is inputted from outside the IC card.

23. (Amended) A program writable IC card according to claim 22, further comprising:

a connector which inputs said encrypted second program from outside the IC card.

24. (Twice Amended) A program writable IC card comprising:

a microprocessor;

a first memory which stores a first program which is executed by said microprocessor and a second program, executable by said microprocessor, for decrypting an encrypted program,

wherein said first memory is a read only memory (ROM) which is not re-writable;

a second memory which is able to store a third program; and

an input unit which inputs an encrypted third program, which has been encrypted based on an encryption key, from outside the IC card,

wherein said microprocessor applies said second program to said encrypted third program inputted by said input unit, stores a decrypted third program which is executable by said microprocessor in said second memory and then executes said decrypted third program stored in said second memory.

25. (Amended) A program writable IC card according to claim 24, wherein said second program has a function for controlling the writing of a program in said second memory, and said microprocessor writes said decrypted third program in said second memory according to said second program.

26. (Twice Amended) A program writable IC card, comprising:
a microprocessor;
a first memory which stores a first program having a decryption function which is executed by said microprocessor,
wherein said first memory is a read only memory (ROM) which is not re-writable; and
a second memory which is able to store a second program,
wherein said microprocessor applies said decryption function to an encrypted second program, which has been encrypted based on an encryption key, according to said first program and then stores a decrypted second program which is executable by said microprocessor in said second memory, wherein said encrypted second program is initially supplied from outside the IC card.

27. (Amended) A program writable IC card according to claim 20, wherein said first program performs an original function of the IC card.

28. (Amended) A program writable IC card according to claim 22, wherein said first program performs an original function of the IC card.

29. (Amended) A program writable IC card according to claim 24, wherein said first program performs an original function of the IC card.

30. (Amended) A program writable IC card according to claim 26, wherein said first program performs an original function of the IC card.

31. (Amended) A program writable IC card according to claim 20, wherein said first program is an IC card function program for realizing an original function of the IC card.

32. (Amended) A program writable IC card according to claim 22, wherein said first program is an IC card function program for realizing an original function of the IC card.

33. (Amended) A program writable IC card according to claim 24, wherein said first program is an IC card function program original for realizing an original function of the IC card.

34. (Amended) A program writable IC card according to claim 26, wherein said first program is an IC card function program for realizing an original function of the IC card.

35. (Amended) A program writable IC card according to claim 20, wherein said first memory is Read Only Memory which is unable to rewrite.

36. (Amended) A program writable IC card according to claim 22, wherein said first memory is Read Only Memory which is unable to rewrite.

37. (Amended) A program writable IC card according to claim 24, wherein said first memory is Read Only Memory which is unable to rewrite.

38. (Amended) A program writable IC card according to claim 26, wherein said first memory is Read Only Memory which is unable to rewrite.

51. (Amended) A program writable IC card according to claim 20, wherein said first program has been stored before said second program is stored in said second memory, and wherein said second program is a new program.

52. (Amended) A program writable IC card according to claim 22, wherein said first program has been stored before said second program is stored in said second memory, and wherein said second program is a new program.

53. (Amended) A program writable IC card according to claim 24, wherein said first program has been stored before said second program is stored in said second memory, and wherein said third program is a new program.

54. (Amended) A program writable IC card according to claim 26, wherein

said first program has been stored before said second program is stored in said second memory, and wherein said third program is a new program.

55. (Amended) A program writable IC card according to claim 20, wherein said second memory can be written only once.

56. (Amended) A program writable IC card according to claim 22, wherein said second memory can be written only once.

57. (Amended) A program writable IC card according to claim 24, wherein said third memory can be written only once.

58. (Amended) A program writable IC card according to claim 26, wherein said second memory can be written only once.

71. (Twice Amended) A processing method for a program writable IC card having a microprocessor, a first memory which stores both a first program which is executed by said microprocessor and a decryption program having a decryption function, wherein said first memory is a read only memory (ROM) which is not re-writable, and a second memory, said processing method comprising:

inputting an encrypted second program, which has been encrypted based on an encryption key, from outside the IC card;

decrypting said encrypted second program according to said decryption program; and

storing a decrypted second program in said second memory, said

decrypted second program being executable by said microprocessor.

72. (Twice Amended) A processing method according to claim 71, said processing method further comprising:

executing said decrypted second program after storing said decrypted second program in said second memory.

73. (Amended) A processing method for a program writable IC card having a microprocessor, a first memory which stores both a first program which is executed by said microprocessor and a decryption program having a decryption function, wherein said first memory is a read only memory (ROM) which is not re-writable, a second memory;, and an input unit, said processing method comprising:

inputting from an external device an encrypted second program, which has been encrypted based on an encryption key, via said input unit;

decrypting said encrypted second program according to said decryption program;

storing a decrypted second program in said second memory, said decrypted second program being executable by said microprocessor; and

executing said decrypted second program stored in said second memory.

74. (Twice Amended) A processing method for a program writable IC card having a microprocessor, a first memory which stores a decryption program executed by said microprocessor, wherein said first memory is a read only memory (ROM) which is not re-writable, and a second memory, said processing method comprising:

inputting an encrypted second program, which has been encrypted based on an encryption key, from an external device;

decrypting said encrypted second program according to said decryption program; and

storing a decrypted second program in said second memory, wherein said second memory can be written only once, and wherein said decrypted second program is executable by said microprocessor.

75. (Twice Amended) A writing method for an IC card having a microprocessor, a ROM device which stores a first program which is executed by said microprocessor, a write control program having a decryption function, and a writable memory, said writing method comprising:

inputting an encrypted second program, which has been encrypted based on an encryption key, from an external device;

decrypting said encrypted second program according to said write control program; and

storing a decrypted second program in said writable memory according to said write control program, said decrypted second program being executable by said microprocessor.

76. (Amended) The writing method for an IC card according to claim 75, said writing method further comprising:

executing said decrypted second program after storing said decrypted second program in said writable memory.

77. (Amended) A writing method for an IC card having a microprocessor, a ROM device which stores both a first program which is executed by said microprocessor, a decryption program having a decryption function, a writable memory, and an input unit, said writing method comprising:

inputting an encrypted second program, which has been encrypted based on an encryption key, via said input unit from an external device;

decrypting said encrypted second program according to said decryption program;

storing a decrypted second program in said writable memory, said decrypted second program being executable by said microprocessor; and
executing said decrypted second program stored in said writable memory.

78. (Amended) A processing method for a program writable IC card according to claim 71, wherein said first program performs an original function of the IC card.

79. (Amended) A processing method for a program writable IC card according to claim 73, wherein said first program performs an original function of the IC card.

80. (Amended) A processing method for a program writable IC card according to claim 74, wherein said first program performs an original function of the IC card.

81. (Amended) A writing method for an IC card according to claim 75, wherein said first program performs an original function of the IC card.

82. (Amended) A writing method for an IC card according to claim 77, wherein said first program performs an original function of the IC card.

83. (Amended) A processing method for a program writable IC card according to claim 71, wherein said first program is an IC card function program for realizing an original function of the IC card.

84. (Amended) A processing method for a program writable IC card according to claim 73, wherein said first program is an IC card function program for realizing an original function of the IC card.

85. (Amended) A processing method for a program writable IC card according to claim 74, wherein said first program is an IC card function program for realizing an original function of the IC card.

86. (Amended) A writing method for an IC card according to claim 75, wherein said first program is an IC card function program for realizing an original function of the IC card.

87. (Amended) A writing method for an IC card according to claim 77, wherein said first program is an IC card function program for realizing an original

function of the IC card.

93. (Amended) A processing method of a program writable IC card according to claim 80, wherein said second memory can be written only once.

94. (Amended) A writing method for an IC card according to claim 76, wherein said writable memory can be written only once.